Title	オンライン計算に於ける領域計算量 (数理情報科学の基礎理論と応用)
Author(s)	町田, 元; 笠井, 琢美
Citation	数理解析研究所講究録 (1981), 421: 163-179
Issue Date	1981-03
URL	http://hdl.handle.net/2433/102543
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
421 巻 1981 年 163-179

オンライン計算に於ける領域計算量

電通大　　町田　元
笠井琢美

1.　はじめに

計算量の理論（計算の複雑さの理論）に於いて，具体的に与えられた何らかの問題に対して，その計算量（時間，領域など）のよい下界を求めることは重要であり，また興味深い問題でもある。近年多くの研究がなされているが，計算モデルとして通常のオフライン・チューリング機械を考えると，この問題は極めて難しく，対角線論法のほかには有効な手法はほとんど知られていない。

これに対して，計算モデルを，入力テープのヘッドの動きを1方向のみに制限した，オンライン・チューリング機械に限定して考えると，いくつかの問題に対して計算量の自明でない下界を求めることが可能となる。Hartmanis と Shank（[4]，[5]）はオンライン・チューリング機械のもとで素数の認識問題を考察し，この問題は領域量 n を必要とすることを

示した。また，Lewis，Stearns と Hartmanis [6] はある特定の文脈自由言語に対してその言語の認識問題の領域計算量が n であることを示し，Gallaire [3] は別の文脈自由言語についてその認識問題が $n^2/\log n$ 時間を必要とすることを示した。さらに，Paterson，Fischer と Meyer [7] はオンラインのほかにいくつかの制約のついた計算モデルの上で2進数の乗算に必要な時間計算量を考察した。

本論文では，このような流れを引きつぎ，いくつかの具体的に与えられた集合（問題）および関数について，オンライン・チューリング機械のもとでの領域計算量の下界について考察する。計算モデル（チューリング機械）に対する制約はオンラインであるということだけで，そのほかには特に制限を加えない。取り上げるおもな問題および関数は次のようなものである。

(i) 3のベキ乗を表わす2進列全体の集合。

(ii) 整数（2進数）の乗算。

(iii) 中置記法で表わされた算術式の Polish記法への変換。

主要結果として，(i)，(ii)，(iii) のいずれもちょうど n のオーダーの領域を必要とすることを示す。また，(i) に対する結果から直ちに，2進数を3進数に変換する関数も n の領域を必要とすることが導かれる。一方，(ii) の証明に関連して，

非決定性オンライン・チューリング機械で $O(\log n)$ 領域で認識可能な集合のクラスは，決定性オンライン・チューリング機械で $O(\log n)$ 領域で認識可能な集合のクラスを真に含むことなども示す。

本稿では，ページ数の制限のため，論旨の筋道に直接関与しない補題の証明は省略した。省略した証明のなかには，主定理の証明の本質的な部分を含むものもある。

2. 準　備

まず，オンライン・チューリング機械，$S(n)$ 領域計算可能，$S(n)$ 領域必要，など本稿に於ける考察の基礎となる概念を定義する。

定義. オンライン・チューリング機械とは，入力テープ，出力テープ各1本と有限個の（半無限）補助テープとから成るチューリング機械で，入力テープと出力テープに対する各ヘッドの動きが1方向のみしか許されていないもののことである（補助テープに対するヘッドはどちらの方向に動いてもよい）。

今後，チューリング機械は，オンライン・チューリング機械しか考えないので，単にチューリング機械と書いてもオンライン・チューリング機械を表わすこととする。

定義. Σ_1とΣ_2を任意のアルファベットとする。関数$f:\Sigma_1^* \to \Sigma_2^*$および$S:\mathbb{N}\to\mathbb{N}$に対して，$f$が$S(n)$領域計算可能であるとは，次の(1)〜(3)を満たすチューリング機械Mが存在することである。

(1) Mの入力アルファベットはΣ_1，出力アルファベットはΣ_2である。

(2) 任意の入力$w\in\Sigma_1^*$に対して，Mは出力テープ上に$f(w)$を出力して，停止する。

(3) 任意の入力$w\in\Sigma_1^*$に対して，wの長さ$|w|$をnとおくとき，Mのどの補助テープについても計算の過程で高々$S(n)$個のセルしか用いられない。

また，Σ_1^*の部分集合について，Aが$S(n)$領域認識可能であるとは，Aの特性関数C_Aが$S(n)$領域計算可能であることをいう。ただし，このとき$\Sigma_2=\{0,1\}$で，出力は入力列をすべて読み終わったときにのみ与えられるものとする。

定義. fおよびSを上と同様とする。

$$\inf_{n\to\infty}\frac{S'(n)}{S(n)} = 0$$

を満たすいかなる関数$S':\mathbb{N}\to\mathbb{N}$についても$f$が$S'(n)$領域計算可能でないとき，$f$は$S(n)$の領域を必要とする（または，$f$の領域計算量は$\Omega(S(n))$である）という。また，集

合Aについても，Aの特性関数C_Aが$S(n)$の領域を必要とするとき，Aは<u>$S(n)$の領域を必要とする</u>（または，Aの<u>領域計算量は$\Omega(S(n))$</u>である）という。

<u>定義</u> Σ_1とΣ_2を任意のアルファベットとする。部分集合$A \subseteq \Sigma_1^*$，$B \subseteq \Sigma_2^*$および関数$f: \Sigma_1^* \to \Sigma_2^*$について，任意の$w \in \Sigma_1^*$に対して，

$$w \in A \iff f(w) \in B$$

が成り立つとき，Aはfによって Bに<u>還元可能</u>であるという。

次の２つの補題は定義から直ちに得られる。

<u>補題2．1</u> Σをアルファベットとし，$A \subseteq \Sigma^*$とする。このとき，Aが正規集合であることと，Aが$O(1)$領域認識可能であることとは同値である。

<u>補題2．2</u> Σをアルファベットとし，A，BをΣ^*の部分集合とする。Aが$S_1(n)$領域認識可能であり，Bが$S_2(n)$領域認識可能であれば，$A \cup B$および$A \cap B$はいずれも$S_1(n)+S_2(n)$領域認識可能である。

<u>記法</u> これ以後，$\Sigma = \{0, 1\}$とおく。また，Σ^+の元$w = a_1 a_2 \cdots\cdots a_n$（$n > 0$）に対して，wが表わす2進数（ただし，左端を低位，右端を高位のビットとする）を$[w]$と記す。すなわち，

$$[w] = \sum_{i=1}^{n} a_i \cdot 2^{i-1}$$

である。

3. 下界を求めるための手法

次節以後，いくつかの問題，関数についてその領域計算量の下界がnであることを示すが，それらの証明で用いられる基本的な考え方は次の補題で表わされる。

補題3．1 Γをアルファベットとし，AをΓ^*の任意の部分集合とする。各$n \in \mathbb{N}$に対して$A^{(n)}$を集合

$$\{u \in \Gamma^* \mid |u|=n,\ \text{ある}\ v \in \Gamma^*\ \text{が存在して}\ uv \in A\}$$

の1つの部分集合とする。このとき，次の2条件が満たされるならば，集合Aはnの領域を必要とする。

(1) 定数cおよびn_0が存在して，任意の$n > n_0$に対して，

$$|A^{(n)}| \geq 2^{n-c}.$$

(2) $A^{(n)}$の中の任意の相異なる2元u_1，u_2に対して，v($\in \Gamma^*$)が存在して，

$$u_1 v \in A \quad \text{かつ} \quad u_2 v \notin A$$

$$\text{または}\ u_1 v \notin A \quad \text{かつ} \quad u_2 v \in A$$

略証．入力を途中まで読んだ時の情報量を評価することによって得られる。 □

一方，すでに下界が知られている集合を媒介にして還元可能性を用いて別の集合の下界を求めることもできる。そのと

き用いられる補題は次のものである。

補題３．２　Σ_1，Σ_2をアルファベットとし，$A \subseteq \Sigma_1^*$，$B \subseteq \Sigma_2^*$，$f : \Sigma_1^* \to \Sigma_2^*$とする。AはBにfによって還元可能であり，Bは$S_1(n)$領域認識可能，fは$S_2(n)$領域計算可能とすると，Aは$S_1(n)+S_2(n)$領域認識可能である。

４．３のベキ乗を表わす２進列の集合の認識

３のベキ乗を表わす２進列全体から成る集合をTとおく。すなわち，

$$T = \{ w \in \Sigma^* \cdot 1 \mid [w] = 3^k,\ k \in \mathbb{N} \}.$$

Tが$O(n)$領域認識可能であることは容易にわかる。本節の目的は，次の定理を得ることである。

定理４．１　集合Tはnの領域を必要とする。

補題３．１を用いて定理４．１を証明する。任意の$k \in \mathbb{N}$に対して，3^kを表わす２進列（$\in \Sigma^* \cdot 1$）をw_kとおく。すなわち，

$$[w_k] = 3^k.$$

従って，

$$T = \{ w_k \mid k \in \mathbb{N} \}$$

となる。さらに，$n \in \mathbb{N}$に対して，Tの長さn以上の元w_kの先頭n文字からなる列を$w_k^{(n)}$とし，それらの列全体から

なる集合を$T^{(n)}$とおく。従って，

$$T^{(n)} = \{ w_k^{(n)} \mid k \in \mathbb{N},\ |w_k^{(n)}| = n,\ (\exists v \in \Sigma^*)\, w_k^{(n)} \cdot v = w_k \}.$$

$T^{(n)}$の元が表わす整数を（kの）順に並べた数列

$$[w_{k_n}^{(n)}],\ [w_{k_n+1}^{(n)}],\ [w_{k_n+2}^{(n)}],\ \cdots$$

を考えると，これは周期列である（ここで，k_nは$|w_k| \geqq n$を満たす最小のkである）。この数列の周期を$\pi(n)$とおく。すなわち，任意の$n \in \mathbb{N}$，$k \geqq k_n$に対して，

$$[w_{k+\pi(n)}^{(n)}] = [w_k^{(n)}]$$

であるが，この$\pi(n)$について次の補題が成り立つ。

<u>補題4．2</u>　任意の$n \geqq 3$に対して，$\pi(n) = 2^{n-2}$．

<u>証明</u>．略．

<u>系</u>．$n \geqq 3$のとき，$|T^{(n)}| = 2^{n-2}$.

<u>定理4．1の証明</u>．T，$T^{(n)}$を各々補題3．1に於けるA，$A^{(n)}$とする。上の系より$T^{(n)}$が(1)を満たすことが示される。(2)はTの定義から明らかである。（$|T \cap \Sigma^n| \leqq 1$に注意。）

次に，2進数を3進数に変換する関数φもnの領域を必要とすることを示す。$\Delta = \{0, 1, 2\}$とおき，任意の$w \in \Delta^*$に対して$[w]_3$をwに対応する3進数とする。関数φ：$\Sigma^* \cdot 1 \to \Delta^* \cdot \{1, 2\}$を次のように定める。

$$\varphi(x) = y \iff [x] = [y]_3$$

定理４．３　関数φは，nの領域を必要とする。

証明　$B = \{ w \in \Delta^* \cdot \{1,2\} \mid [w]_3 = 3^k ,\ k \in \mathbb{N} \}$

とおくと，Bは正規集合 0^*1 であるから $O(1)$ 領域認識可能である（補題２．１）。TはφによってBに還元可能である。よって，定理４．１と補題３．２より，この定理が証明される。　□

５．整数の乗算

本節では，整数の乗算がnの領域を必要とすることを示す。

記法　２節でΣ^+の元wに対して，wに対応する整数を示す$[w]$という記法を定めた。逆に，正整数nに対して，nに２進数列 w（$\in \Sigma^* \cdot 1$）（但し，左側が低位，右側が高位で，最高位ビットの最右端は１）を $]w[$ と記す。すなわち，

$]n[= a_1 a_2 \cdots a_k$ $(a_k = 1)$ ならば，

$$n = \sum_{i=1}^{k} a_i \cdot 2^{i-1}$$

である。便宜上，$]0[= 0$ とおく。任意の自然数nに対して，　$[(]n[)] = n$　が成り立つ。

また，$\bar{\Sigma} = \Sigma \cup \{ ¢ \}$ $(¢ \notin \Sigma)$ とおく。Σ^*の任意の２元 $x = a_1 a_2 \cdots a_m$，$y = b_1 b_2 \cdots b_n$ に対して，

$$x \# y = a_1 b_1 a_2 b_2 \cdots a_l b_l$$

と定める。ただし，$l = \max\{m, n\}$ であり，$m < n$ なら

ば $a_{m+1} = \cdots = a_\ell = ¢$ ，$m > n$ ならば $b_{n+1} = \cdots = b_\ell = ¢$ である。以上の準備のもとに乗算 MULT：$\Sigma^* \to \Sigma^*$ を，次のように定める。

$$\mathrm{MULT}(w) = \begin{cases}](([x] * [y]))[& \text{ある } x,\ y \in \Sigma^* \text{ に対して，} \\ & w = x \# y \text{ となるとき} \\ \text{定義されない} & \text{それ以外のとき} \end{cases}$$

ここで，$*$ は通常の整数の乗算を表わす。すなわち，MULT は２つの２進数を各々下位の桁から読み，それらの積を下位の桁から出力する自然な乗算である。

<u>定理５．１</u>　乗算 MULT は，n の領域を必要とする。

この定理の証明のため，平方数を与える関数 SQR：$\Sigma^* \to \Sigma^*$ を次のように定義する。任意の $w \in \Sigma^*$ に対して，

$$\mathrm{SQR}(w) =]([w]^2)[.$$

すなわち，　$[\mathrm{SQR}(w)] = [w]^2$.

<u>補題５．２</u>　関数 $S : \mathbb{N} \to \mathbb{N}$ に対して，MULT が $S(n)$ 領域計算可能であることと，SQR が $S(n)$ 領域計算可能であることは同値である。

<u>証明</u>　MULT が $S(n)$ 領域計算可能であれば，SQR もそうであることは明らか。逆に，SQR が $S(n)$ 領域計算可能であるとする。任意の整数 a，b に対して，

$$a * b = \{(a+b)^2 - (a-b)^2\} / 4$$

が成り立つことと，加算，減算が $O(1)$ 領域で計算可能であることから，MULT も $S(n)$ 領域計算可能となる。 □

定理５．１を証明するためには，次の定理を示せばよい。

定理５．３　SQRは n の領域を必要とする。

この定理は，次のいくつかの補題を用いて証明される。まず，集合Ａ，Ｂ（$\subseteq \Sigma^*$）を次のように定義する。

$A = \{ w \in \Sigma^* \mid w = 1^{e_1} 0^{f_1} 1^{e_2} 0^{f_2} \cdots 0^{f_t} 1^{e_{t+1}}$

（$e_1, \cdots, e_{t+1}, f_1, \cdots, f_t > 0$，$t \geq 3$）と表わされ，$f_1$，$f_2$，…，$f_t$ の中で３番目に大きなものの１つを f_s（$1 \leq s \leq t$）とすると，部分列 $1^{e_{s+2}} 0^{f_{s+2}} \cdots 0^{f_t} 1^{e_{t+1}}$ の左端から右に f_{s+1} 番目の文字は１である $\}$.

$B = \{ w \in \Sigma^* \mid w = 1w'1$ かつ $SQR(w) \in A \}$.

補題５．４　Ａは $\log n$ 領域認識可能である。

略証　３本の補助テープを用いて，それまでに入力された（両端を１ではさまれた）０だけから成る部分列のうち，最も長い列，２番目に長い列，３番目に長い列のそれぞれの長さとそれに対応する“f_{s+1} 番目のビット”の内容とを記憶しておけばよい。 □

補題５．５　Ｂは n の領域を必要とする。

この証明も補題３．１をもとにしてなされる。任意の $n \in$

$\mathbb{N}$に対して，

$B^{(n)} = \{u \mid u \in 1\Sigma^*1,\ |u| = n,$ ある $v \in \Sigma^*$ に対して $uv \in B\}.$

とおく。次の2つの補題を示せばよい。

補題5．6　任意の $n \geqq 2$ に対して，$|B^{(n)}| = 2^{n-2}$．

補題5．7　$n > 2$ とする。$B^{(n)}$ の中の任意の相異なる2元 u_1，u_2 に対して，$v \in \Sigma^*$ が存在して，

$$u_1 v \in B \text{ かつ } u_2 v \notin B$$

$$\text{または } u_1 v \notin B \text{ かつ } u_2 v \in B$$

となる。

定理5．3の証明　SQRが，

$$\inf_{n \to \infty} \frac{S(n)}{n} = 0$$

を満たすSについて，$S(n)$ 領域計算可能であるとする。すると，Bの認識がやはり $S(n) + \log n$ 領域でできてしまうことが次のようにしてわかる。

入力列 w に対して，w を2乗する。これはSQRによって $S(n)$ の領域でできる。次に，得られる列 u（$[u] = [w]^2$）がAに属するかどうかを調べる。これは，$\log n$ の領域でできる（補題5．4）。従って，Bは $S(n) + \log n$ 領域認識可能となり，補題5．5に反する。

すなわち，SQRも n の領域を必要とする。□

以上で，最初に定めた乗算MULTがnの領域を必要とすることの証明が終わったが，2つ注意をしておく。

1. MULTは，nの領域で計算可能である。

2. 以上の結果は，乗算(MULT)の定義のしかたに特別に依存するものではない。乗算の定義を別のものに変えても，"自然"なものである限り，同様の結果が得られる。

6. オンライン計算に関する2つの性質

集合C（$\subseteq \Sigma^*$）を次のように定める。

$C = \{ w \in \Sigma^* \mid w = u \cdot 1 \cdot 0^i \cdot 1$ （$|u| \geq i$，$i \in \mathbb{N}$）と表わされ，uの右からi番目のビットは1である$\}$.

Cについて，次のような性質が成り立つ。

補題6.1 (i) Cはnの領域を必要とする。

(ii) Cの逆語の全体C^Rは$\log n$領域認識可能である。

(iii) Cは非決定性（オンライン）チューリング機械を用いると，$\log n$領域で認識可能である。

この補題から次の2つの定理が得られる。

定理6.2 $\log n$領域で認識可能な言語のクラスは，逆語

をとる操作に関して閉じていない。

決定性（非決定性）チューリング機械により $\log n$ 領域で認識可能な言語のクラスを ON-LINE DLOG（NLOG）SPACE と表わす。

定理 6．3　ON-LINE DLOG SPACE $\subsetneq$ ON-LINE NLOG SPACE

7．算術式の変換

最後に，算術式を中置記法から後置記法（Polish 記法）に変換する問題を考える。

定義　$\mathcal{J}$，$\mathcal{O}$ をアルファベットとし，$\mathcal{J} \cap \mathcal{O} = \phi$ とする。$\Gamma = \mathcal{J} \cup \mathcal{O}$，$\Delta = \Gamma \cup \{(,)\}$ とおく。Γ 上の中置算術式の集合 AEXP（$\subseteq \Delta^*$）は，次の i)，ii) を満たす最小の集合である。

i)　$\mathcal{J} \subseteq$ AEXP，

ii)　$x, y \in$ AEXP，$\sigma \in \mathcal{O}$ のとき $(x\sigma y) \in$ AEXP．

Γ 上の後置算術式の集合 POSTEXP（$\subseteq \Gamma^*$）は，次の i)，ii) を満たす最小の集合である。

i)　$\mathcal{J} \subseteq$ POSTEXP，

ii)　x，$y \in$ POSTEXP，$\sigma \in \mathcal{O}$ のとき $xy\sigma \in$ POSTEXP．

次の 3 つの条件を満足する関数 $\psi : \Delta^* \to \Gamma^*$ を算術式変換関数（または，目的コード生成関数）と呼ぶ。

i)　$a \in \mathcal{J}$ に対して，$\psi(a) = a$，

ii) $x, y \in$ AEXP, $\sigma \in \mathcal{O}$ に対して, $\psi((x \sigma y)) = \psi(x)\psi(y)\sigma$,

iii) $x \notin$ AEXP ならば $\psi(x) \notin$ POSTEXP.

定理７．１　算術式変換関数ψはnの領域を必要とする。

この定理を示すために，予備的考察を行なう。$\Sigma = \{0, 1\}$ とする。

補題７．２　i)集合 $A = \{ w \mathrm{¢} w^R \mathrm{¢} \mid w \in \Sigma^* \}$ は n の領域を必要とする。

ii)集合 $B = \{ 0^n 1^n \mid n \in \mathbb{N} \}$ は $\log n$ の領域を必要とする。

((i)は，Lewis, Stearns と Hartmanis [6] による。もちろん，本稿の補題３．１を用いれば容易である。)

定理７．３　POSTEXP は，$\log n$ 領域認識可能であり，また，$\log n$ 領域を必要とする(すなわち，$\log n$ の領域が必要かつ十分である)。

略証　$\log n$ 領域必要なことは次のように示される。補題３．２と補題７．２(ii)より，集合 $\{ a^{2n} b^n \mid n \in \mathbb{N} \}$ が $\log n$ 領域を必要とすることが示される。$a \in \mathcal{T}$，$b \in \mathcal{O}$ とすると，

$$\mathrm{POSTEXP} \cap a^* b^* = \{ a^{2n} b^n \mid n \in \mathbb{N} \}$$

である。よって，補題２．１と２．２より POSTEXP は $\log n$ の領域を必要とする。　□

定理７．４　AEXPは，n領域認識可能であり，また，n領域を必要とする(すなわち，nの領域が必要かつ十分である)。

略証. n領域を必要とすることは，O(1) 領域計算可能な関数fを構成することによって，補題7．2(i)の集合がfによってAEXPに還元可能であることを示すことによって証明される。 □

定理7．1の証明　AEXPはΨによってPOSTEXPに還元可能であるから，補題3．2，定理7．3，7．4より明らか。

謝辞. 本稿と関係なく日頃御世話頂く電気通信大学計算機科学科の諸氏，諸嬢，とくに西澤輝泰，樋川知子，竹元裕子各氏（ちなみに，竹元女史は本講究録中の"Lisp プログラム自動合成の一システム"の執筆者永井雅人氏の実姉である）に深甚の感謝の意を表したい。また，数ページにわたる難解な草稿を忍耐強く清書して頂いた同大学戸田誠之助氏に深く感謝する。

怨辞. 本稿に関し，日頃有害無益な難癖をつけていただく相模工大岩田茂樹先生に怨念をこめて御礼を申し上げたい。

参考文献

1. Aho, A. V., J. E. Hopcroft and J. D. Ullman, The Design and Analysis of Computer Algorithms, Addison-Wesley, Reading, Mass., (1974).
2. Fischer, M. J., and L. J. Stockmeyer, Fast on-line integer multiplication, J. Comput. System Sci. 9, 317-331 (1974).
3. Gallaire, H., Recognition time of context-free languages by on-line Turing machines, Inform. Contr. 15, 288-295 (1969).
4. Hartmanis, J., and H. Shank, On the recognition of primes by automata, J. Assoc. Comput. Machinery 15, 382-389 (1968).
5. Hartmanis, J., and H. Shank, Two memory bounds for the recognition of primes by automata, Math. Systems Theory 3, 125-129 (1969).
6. Lewis, P. M. II, R. E. Stearns, and J. Hartmanis, Memory bounds for recognition of context-free and context-sensitive languages, IEEE Conference Record 6th Annual Symposium on Switching Circuit Thory and Logic Design, 191-202 (1965).
7. Paterson, M. S., M. J. Fischer, and A. R. Meyer, An improved overlap argument for on-line multiplication, in Complexity of Computation (SIAM-AMS Proceedings, Vol. 7), R. M. Karp, Ed., American Mathematical Society, Providence, Rhode Island, 97-111 (1974).